Set Task Electronic Template – Unit 11

Task A - Activity 2 Template: Cyber security plan for the networked system

Use the section headings below for each protection measure.
1) Threat(s) addressed by the protection measure
2) Details of action(s) to be taken
3) Reasons for the actions
4) Overview of constraints – technical and financial
5) Overview of legal responsibilities
6) Overview of usability of the system
7) Outline cost-benefit
8) Test plan

Test plan

Test No	Test description	Expected outcome	Possible further action following test
1	The password set for the remote access method is strong/weak. (via VPN)	If the password set is weak then it should be	Password should only be accepted if its strong, otherwise system should be configured.
2	Check VPN security setting using IP leak test tool	Leak tool will show if there is a lack of configuration resulting in flags on the system.	Check the VPN is active using the OpenVPN protocol software which can grant protective security.
3	Attempting to access services other than browsing the internet	Cannot connect to other services or areas.	Reconfigure software and ports accordingly.
4	A login to the VPN server using the default ports	The default ports would fail and the configured ports will give access to the server.	Reconfigure the software and the ports required.
5	Visitor SSID, visitor WAP and attempt to access the EPE network	Visitors cannot enter restricted areas, only places allowed.	The system should beep and flag on the system.
6	Access the system attempt of hacking or bypassing the control door system	An alarm to alert the security department that a break in is taking place	The CCTV system should pick up any activities around the control door.
7	Attempt login to staff	Login screen asking for password should be displayed.	Repeat the test with each staff WAP to

	WAP	Login succeeds with correct password.	ensure that WAP2 and SSID has been configured correctly on each.
8	Login Staff Network and attempt to access Confidential data files with lack of access rights	Access should be denied	A repeat of the procedure with this with the right of access and the access should be enabled
9	Attempt login from external (outside of the remote access) remote access software	Access should be granted to the remote access server	
10	Attempt staff login to staff WAP, with both listed and unlisted devices	Only listed devices will login	Try this again.
11	Access the system attempt of hacking or bypassing the control door system	CCTV surveillance accruing the video footage recording and announcing intrusion	If access is denied or connects to the wrong device reconfigure and retry.

Protection measure 1
Threat/s addressed 3,1,6,9,11, Attack via main switch, Attack on /theft of client information, Staff and visitors using the same network, Misconfigured firewall, Access the network through remote access VPN.
Actions that need to be taken: Programme or install the firewall if it is not already in the router. Configure the firewall protecting the internet to allow access via the Wi-Fi router required by the remote access method chosen. Per recommendation: change the routers from the default ones. The protected VPN should be used so staff and guest don't use same network. Its important to keep staff network and guest network separate as the passing of confidential information is likely to happen.
Configure router port forwarding the network remote access to the correct VPN server. Configure remote access server and client software to work with the ports opened in the firewall.
Reason for actions: Attacks can happen on VPN as it passes data through a shared network. A firewall is able to block these attacks. Open routers such as guest Wi-Fi and staff Wi-Fi for known software can make the component vulnerable to attack. Everything being directly connected to the main switch causes a threat as server can easily be attacked. Securing access points by making sure Wi-Fi router is updated having a backup of the Wi-Fi settings. environment with cafes bars etc it makes it easier for a third party to see the

username and password which therefore can be used to breach the system. Having a strong password determines both remote access software(VPN) and the typical network login which increases the difficulty of getting network access furthermore passwords can be enforced by software.
Technical: There's minimal setup and configuration tasks are simple.
Legal responsibilities: The data needs to be encrypted and protected under the Data Protection Act.
Usability: Minimum even though the enforcement of strong passwords can cause some login errors.
Cost: The attacking of a system would mean that the security company would need to come out and render the system, therefore costing the company a lot to reconfigure the security system such as the SSID cards and the company would need to rebuild firewalls and systems to protect the website data.

Protection measure 2
Threat/s addressed: 2,4
Actions that need to be taken: To have wireless access points checked to ensure they are configured for the guest and staff Wi-Fi access points.
Configure staff WAP creating a strong password that if it is not already done.
MAC address white list to be used on staff WAP so a guest for example cannot access staff connection of Wireless local network connection.
For each access point the correct SSID and the key must be entered.
Reason for actions:
If staff and guests use the same WAP, guests have the chance of logging in to the staff network and therefore security must be enforced through other ways that can be access rights. A separate, visitor, WAP can be configured so that access to the WAP only allows access to a restricted area of the network, for example the internet.
Having strong passwords on staff WAP increases the difficulty of an intruder getting network access.
The MAC access list means it will only allow pre-approved devices to connect and nothing outside of this. So only the devices designated to the staff would be connected and outsiders such as visitors won't be able to access the network meaning the threat of confidential data will be protected.
Having a misconfigured SSID can have a result in user attempts of connecting to the wrong network, which may result in creating a security alert. A misconfigured WPA2 or key may impact the functionality of network. This can provide a point of weakness for an attacker so that they can access the system.
Technical: Separate WAP requires a minimum setup and configuration being a simple.
MAC white list: A moderate constraint being that the list is a simple source to set up but would need to be mapped out to support all staff WAPs. There is a limit on the size of the list which the WAP will allow (this may not be adequate for all staff devices). Ensuring the list is accurate and updated proves responsibility in case there are frequent changes occurring to the device list.
Financial: Since the WAP being cheap with commercial quality means it likely having MAC list capabilities which are required.
Legal responsibilities: The data needs to be encrypted and protected under the Data Protection Act.

Usability: Is low, however, it can be medium if MAC lists are included. Although, if a password is strong, it means it cannot easily be guessed, so the password may also be hard to remember and make the locking out the system a likely factor.
Cost: As there is a possibility of major impact level of data being lost or manipulated, the costs are likely to be high. Code and input data may have to be re-written to provide the system with adequate information to be continually used.

PROTECTION MEASURE 3
Threat/s addressed: 5
Attack via internet connection
Actions that need to be taken: Install or programme the firewall (that's if it is not already present in the router's system). Firewall needs to be configured which allows access through a port required by the system software chosen.
Reasons for actions: Attacks on ports which are commonly used would cause the disruption of the company's activities and allow a hacker potential access to greater information. A firewall will block these unless the relevant port has been opened. Open ports can cause a more targeted attack. By using strong password and making input data difficult to guess, it reduces the likelihood of a hacker or an attack being successful in bringing down the internet connection.
Technical: there is little setup and configuration making it easy to set up the firewall and protection.
Legal responsibilities: The data needs to be encrypted and protected under the Data Protection Act.
Usability: It will be very usable with the firewall but if an attack was to take place and be successful, the user wouldn't be able to access the system.
Cost: The impact being major means the cost involved would be moderate as the process would require paying for the firewall and bring the connection back online.

PROTECTION MEASURE 4
Threat/s addressed 7,810: Attack on access points such as panel, Card Duplication, Controlled door being hacked or bypassing them
Actions that need to be taken:
Protecting the door which can only be accessed via the card reader may result in the system needing extra security features. So, if the door is accessed by any method other than the card reader, an alert is sent to security and the main system therefore locking all information into an area protected by firewalls, passwords and other security. Also, CCTV cameras fitted into the area to record anyone breaking into the room.
Reasons for actions:
CCTV operators in case someone walks in behind a member of staff who scanned their card. Also, the CCTV would pick up any forced entry to the control room.
Technical: Set up of CCTV is relatively simple.
Financial: High: as fitting alarm would cost getting someone to installed buying the alarm, programming it to link to the security room and the maintenance of it. CCTV installation and cost of CCTV is expensive

Legal responsibilities: High as there is a requirement for maintaining security of client data and office equipment responsible of security for confidential data.
Usability: Once installed accessing the video for CCTV surveillance is easy to access through laptop or mobile.
Cost: The benefit of security of the office overweighs the cost of installation of the cost of set up of surveillance and alarm e.g. even though it is expensive the safety and security of data and equipment is more important.